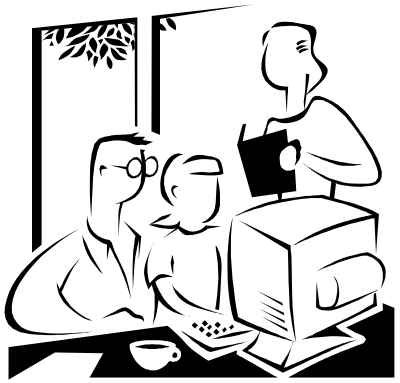
IT Risk Management
-- For Home Computer Users

DFAS
Your Financial Partner @ Work

Audrey Davis
Director, Information Technology & CIO
Defense Finance and Accounting Service

Overview

- Looking at Risk
- Home Computing Threats and Safeguards
  - Viruses/Worms/Trojan Horses
  - SPAM
  - Spyware/Adware
  - Phishing/Identity Theft
  - Online Shopping
  - Children on the Internet
- Summary



Looking at Risk - Basics

- **Risk is the possibility of suffering loss** *(Webster)*
- **Risk is everywhere, in everything we do**
- **Risk and opportunity go hand in hand.**
  - Online activities introduce both risks and opportunities

- **We can not eliminate risk but we can manage it**
  - In Government, my role is to formally authorize operations based on an acceptable security risk. Determining adequate security requires a risk-based approach. (*OMB, NIST, and DoD policy*)
  - Rather than try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them (*DoD 8510.1-M Accreditation Manual*)

Likewise, as home computer users, the more we understand about specific risks, the more effectively we can manage them

Looking at Risk - A Definition and Model

- **Risk** is a threat that exploits some vulnerability that could cause harm to an asset

Risk = Asset * Threat * Vulnerability

PC: Efficiency
Data/files

Yourself: Privacy
Identity
Credit
Confidence

Family: Child
Safety

Viruses/Worms/Trojans SPAM
SpyWare
Phishing
Identity Theft
Shopping Scams
Online Predators

No Firewall
No Anti-virus
Unpatched SW
Unsafe Practice

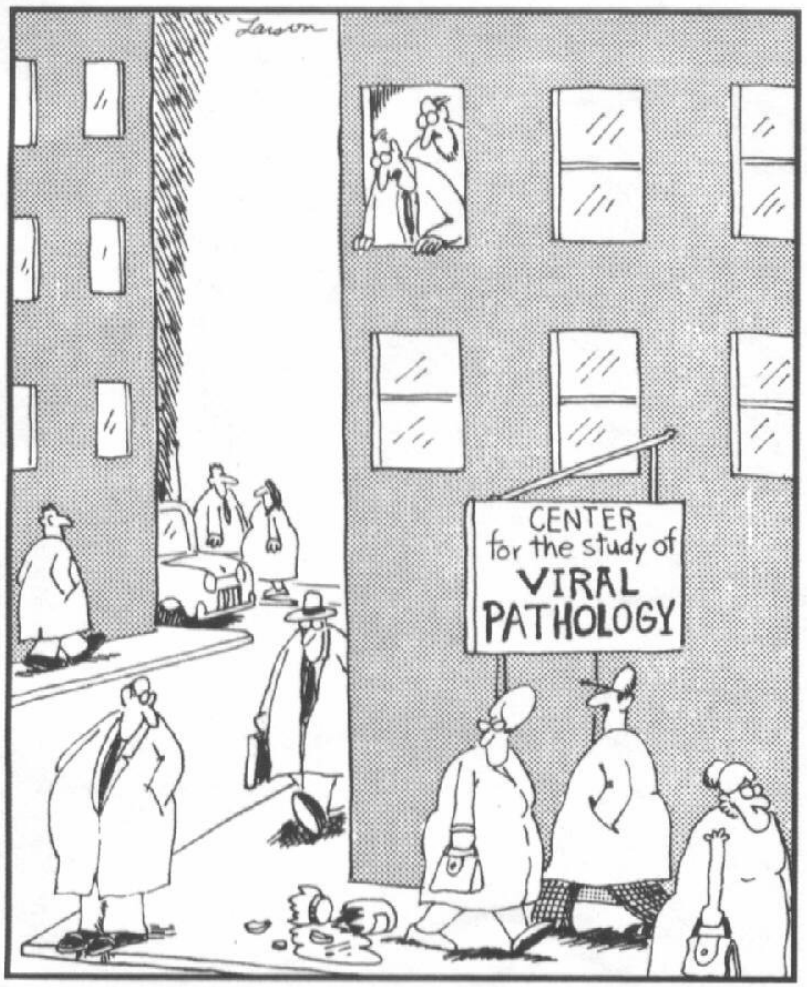
- **Safe**
effect

As you will see, nearly all safeguards available to us for reducing risk are those that reduce or eliminate a vulnerability, especially in the area of unsafe practices.

Viruses/Worms/Trojan Horses

Just as in the physical world, viruses and their brethren in the computer world can be nasty and are spread by infection

Copyright: Larson

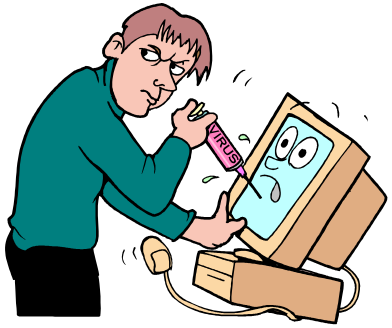


"Uh-oh."

Viruses/Worms/Trojan Horses

- Viruses, worms, and Trojan horses are malicious programs that can cause damage to your computer and information on your computer.

A **virus** is a piece of computer code that attaches itself to a program or file so it can spread. Viruses can damage your software, your hardware, and your files.



A **worm**, one type of a virus, is designed to copy itself from one computer to another, often by e-mail as the transport mechanism. Worms don't need to travel via a "host" program or file.

A **Trojan horse,** another type of virus, is a computer program that appears to be useful but that actually does damage. Victims are lured into willingly opening them.

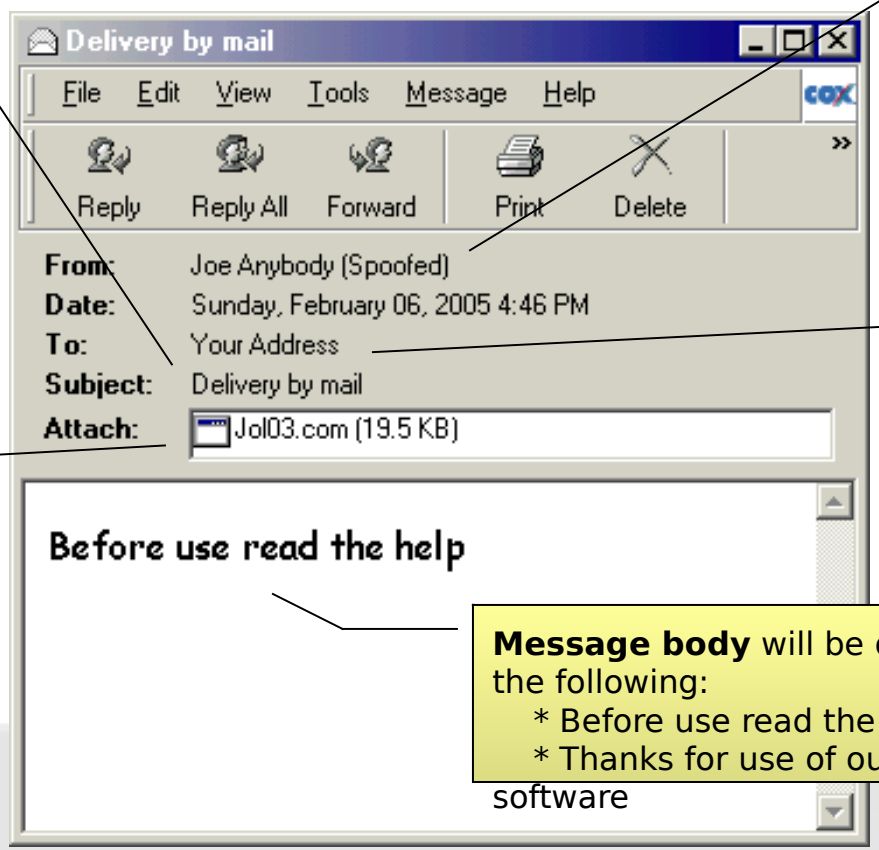
How a Worm-type Virus Works

W32.Beagle.AZ@mm, discovered on January 26, 2005, is a mass-mailing worm-type virus that also spreads through file-sharing networks. The email will have a variable subject and attachment name. The virus is triggered when the attachment is executed by the recipient.

Subject will be one of the following:
* Delivery by mail
* Delivery service mail
* Is delivered mail
* Registration is accepted
* You are made active

Attachment is one of the following:
Jol03, guupd02, siupd02, upd02, viupd02, wsd01, or zupd02

with one of the following **extensions**: .com, .cpl, .exe, or .scr


Delivery by mail
File Edit View Tools Message Help
Reply Reply All Forward Print Delete
From: Joe Anybody (Spoofed)
Date: Sunday, February 06, 2005 4:46 PM
To: Your Address
Subject: Delivery by mail
Attach: Jol03.com (19.5 KB)
Before use read the help

From Address is spoofed. It may be from someone you actually know.

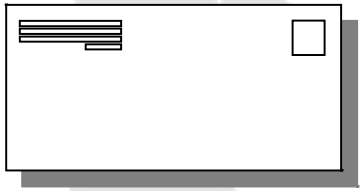
Uses its own SMTP engine to send email messages to addresses collected from the compromised computer.

Message body will be one of the following:
* Before use read the help
* Thanks for use of our software

How Trojan Horses Work

1) Build a Trojan Horse

- Someone writes the code and disguises it as something useful
- Could masquerade as a screen saver, a graphics file, video clip, etc.



2) Deliver the Gift Horse

- Could be posted on a Web site for downloading
- Or sent as an e-mail attachment to intended victim

3) User Accepts the Trojan Horse

- Victim believes the file is a nice “gift” and double-clicks it
- Trojan horse executes and infects victims computer, often installing a backdoor for crackers

4) User’s System Suffers an Attack

- A cracker locates the infected system and accesses
- User’s financial data might be target
- Might use system as a zombie, launching attacks other systems

Trojan Horse Examples

The most damaging Trojan horses are backdoor Trojans, which allow remote access to computers.

Some notable backdoor Trojans still prevalent today a

- **SubSeven** – opens port 1243 and installs server software that lets a cracker control the victim's compute
  Can access files or be used as zombies to launch DoS (denial of service) attacks.
- **NetBus** – installs server software for use with cracker's client software, similar to SubSeven
- **Back Orifice** - like NetBus, includes client and server applications. After a user launches Back Orifice, a cracker can control the user's system.
- **Backdoor.IRC.Flood** - This one installs an instant messaging client that helps crackers gain access.

Viruses/Worms/Trojan Horses Safeguards

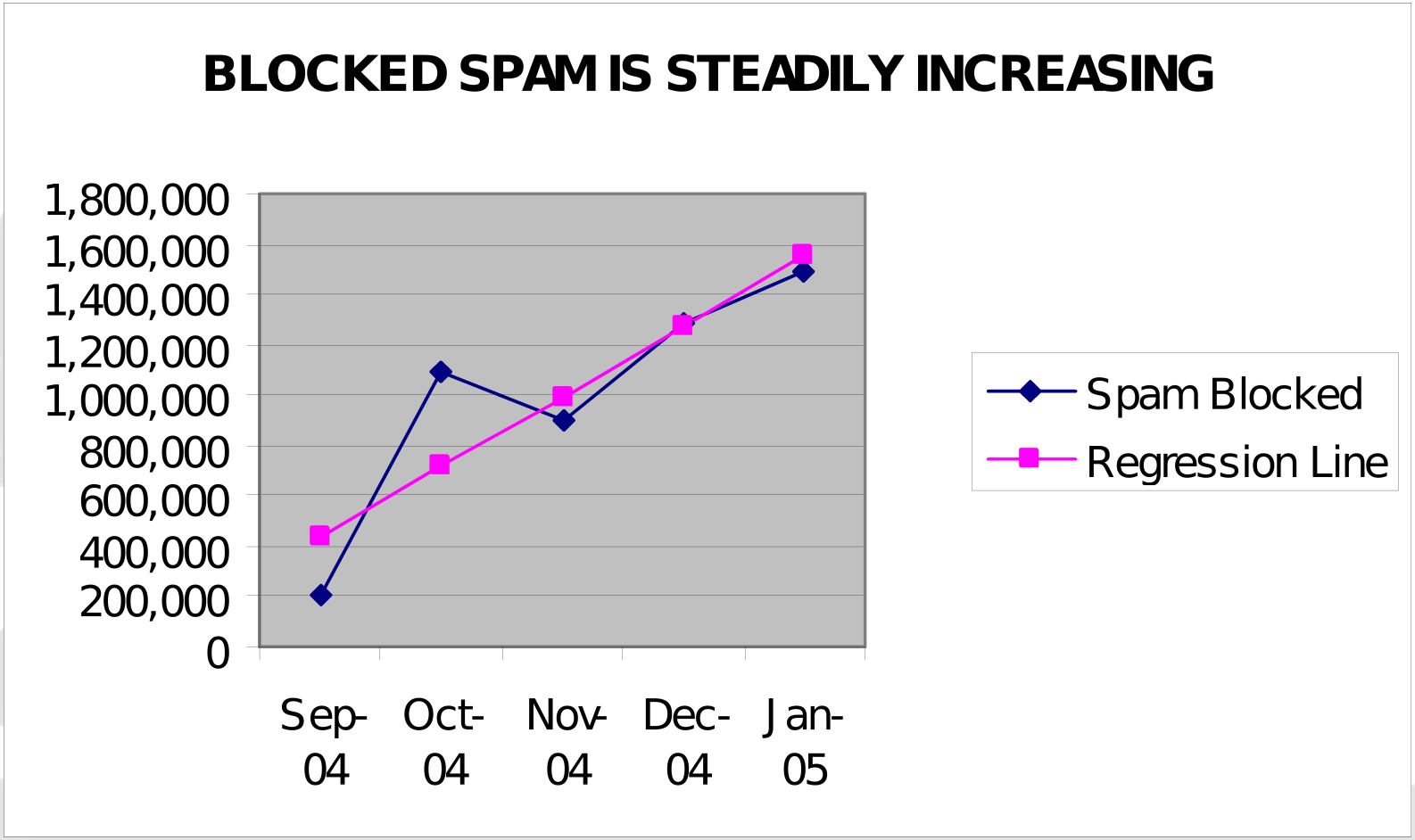
Simple steps for protecting yourself from viruses, worms, and Trojan horses:

- Never open an e-mail attachment from a stranger
- Never open an e-mail attachment from someone you know unless you know exactly what the attachment is
- Be most suspicious of file attachments commonly used to spread viruses, such as ***.com***, ***.vbs***, ***.bat***, ***.exe***, ***.pif*** and ***.scr*** files
- Don't trust displayed file names – can verify via Properties
- Read e-mail messages in plain text
- Install anti-virus software and update pattern files weekly
  - Home use authorized for DoD civilians and military at no cost for ***McAfee***, ***Symantec Norton***, and ***Trend Micro*** anti-virus software
- Always keep your antivirus software up-to-date.
- Backup important files

SPAM

- **E-Mail SPAM (unsolicited e-mail) is not just annoying:**
  - It can be a vehicle for viruses, worms, and Trojan horses
  - Can bring offensive content or fraudulent schemes to your PC
  - Can overwhelm your inbox
- **Despite Federal Can-SPAM Act of 2003, SPAM is still growing**
  - Accounted for about 50 percent of all e-mail in 2003
  - Estimated at 75-80 percent in 2004
- **North Carolina man gets 9-year sentence**
  - Jury convicts spammer under Virginia's SPAM law, which is similar to the federal legislation

DFAS SPAM Metrics Report – January 2005



SPAM Safeguards

- **Do not attempt to use the unsubscribe link**
  - Shows you are a valid account
  - Some of these links will attempt to load Trojan Horses
- **Install and use SPAM filter**
  - *Spamwasher* ($30), *McAfee Internet Security Suite* ($50), and *Norton Internet Security Package* ($70) are examples
- **Do not send email address through chat rooms, instant messaging, Internet bulletin boards or newsgroups**
- **Do not use primary email address for online registration or on e-commerce sites.**
  - Have another email address to use more publicly
- **Do not forward chain email**
  - You will add to the problem
  - And further propagate your own address

Spyware/Adware

- **Spyware** and other unwanted software refers to software that performs certain tasks on your computer, typically without your consent. This may include giving you advertising or collecting personal information about you.

Spyware vs Adware – Know the Difference:

Adware typically spawns targeted pop-up ads as you surf (a.k.a. pestware) while Spyware goes beyond marketing even sometimes to the extent of capturing account information and passwords by logging keystrokes

Spyware/Adware Symptoms

If your computer starts to behave strangely, you may have Spyware or other unwanted software such as Adware

Some common symptoms:

- I see pop-up advertisements all the time.
  - Ads not related to site you are visiting
  - Ads appear as soon as you turn on your computer or when you're not even browsing
- My settings have changed and I can't change them back to the way they were
  - Home page or search page settings change when starting browser or revert back every time you restart your computer
- My Web browser contains additional components that I don't remember downloading
  - Unwanted toolbars to your Web browser that you don't want or need
  - They may return each time you restart your computer
- My computer seems sluggish
  - Spyware often crudely inefficient
  - Tracking your activities can slow down computer
  - Program errors can cause crashes

Spyware/Adware Safeguards

Simple Steps For Protecting Yourself

Step 1: Update Windows and e-mail software

Step 2: Adjust browser security settings

- Set browser security to High
- Block ActiveX
- Add safe web sites to Trusted Sites (IE)

Step 3: Use a personal firewall

- ***Zone Alarm*** (free)
- ***McAfee*** firewall/virus bundle (home use free if DoD civ or mil)
  or you can buy Firewall/Virus/SPAM/Spyware bundle for $50
- ***Norton*** firewall/virus bundle (home use free if DoD civ or mil)
  or you can buy Firewall/Virus/SPAM/Spyware bundle for $70

Step 4: Surf and download more safely

Step 5: Download and install anti-spyware protection.

DFAS Safe Computing Zone recommends

- ***Spybot Search and Destroy*** (free)
- ***Pop Up Killer*** (free)

Phishing for Your Identity - eBay

Take a Quiz:

Phishing e-mails are designed to look like they are sent by legitimate businesses. Can you tell the difference between a fake and the real thing?

Fake or Legitimate?

home | pay | services | site map | help

ID Verify

Dear eBay user,

You are urged to establish your proof of identity with ID Verify - an easy way to help others trust you as their trading partner as our service quality is changing. The process takes about 5 minutes to complete and involves updating your information over a secure connection. When you're successfully verified, you will receive an ID Verify icon in your feedback profile. This feature applies to residents of the United States and U.S. territories (Puerto Rico, US Virgin Islands and Guam), Europe (EU) , Japan and Australia.

Fee: Verification is free of charge and is valid until your name, home address or phone number change.

Click here and ID Verify Now, help us improve the service we are providing to our customers.

Note: After successful verification, you will not be able to modify your contact information for 30 days. Also, the ID Verify icon is used for 3 different verification processes. Verisign provides individual verification on eBay.com.

This is a bogus eBay e-mail that tries to take advantage of eBay's very real ID Verify program. Notice the scammers try to scare you into responding immediately and giving up your personal information. It also asks you to click on a link in the e-mail; this is never a good idea.

Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

Credit for Phishing examples:
Washington Post, 2005

Phishing for Your Identity - Citibank

Take a Quiz:

Phishing e-mails are designed to look like they are sent by legitimate businesses. Can you tell the difference between a fake and the real thing?

Fake or Legitimate?

Security key: qlgarixmqjt

citi

Dear Citibank.com Customer,

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below:
https://web.da-us.citibank.com/cgi-bin/help_desk/verify.asp
AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.

Note: Requests for information will be initiated by Citibank Business Development; this process cannot be externally requested through Customer Support.

brcffq

The key giveaway to this phish is that it asks you to "verify" your account information. Most banks will address their customers by name, whereas this e-mail starts with the salutation "Dear Customer."

Credit for Phishing examples:
Washington Post, 2005

Phishing for Your Identity – Citicards

Take a Quiz:

Phishing e-mails are designed to look like they are sent by legitimate businesses. Can you tell the difference between a fake and the real thing?

Fake or Legitimate?

Dear *****:

Only a select group of customers have qualified for this special opportunity, and we're delighted to count you among them.

Take advantage of this special offer to pay off high rate credit cards at your low Balance Transfer rate today!

But you must act soon... Please visit balancetransfer.accountonline.com before 11-05-04 to take advantage of this offer.

Sincerely,

This is not a phishing scam, though it sure looks like some of the others we've seen. It just shows how difficult it is these days for consumers to tell the difference between phishing scams and legitimate e-mails between companies and their customers.

...re interest expenses with a low balance transfer rate.

Credit for Phishing examples:
Washington Post, 2005

Phishing for Your Identity – eBay (2nd)

Take a Quiz:

Phishing e-mails are designed to look like they are sent by legitimate businesses. Can you tell the difference between a fake and the real thing?

Fake or Legitimate?

Browse
Search
Sell
My eBay
Community
Sign In
Need Help?
Verify Identity now!
We are currently performing regular maintenance of our security measures.
Please sign in twice. Once you signed in second time your ebay account will be automatically verified and updated.
Protecting the security of your eBay auction account is our primary concern,
and we apologize for any inconvenience this may cause.
Comments are welcomed!
Verify your identity
Your personal information will be verified instantly. All the data is protected by the industry standard SSL encryption. Al
information is required and is kept confidential in accordance with eBay's Privacy Policy.
Enter Your Registration Information
User ID
Password
Account type
Seller
Buyer
Name
First Name
M.I.
Last Name
Email
Email password
their respective owners.
Use of this Web site constitutes acceptance of the
eBay User Agreement and Privacy Policy.

This one certainly has all the right graphics for eBay, but closer inspection reveals some sloppiness in grammar. But the major red flag here is eBay and most banks will never ask you for your financial details in an e-mail.

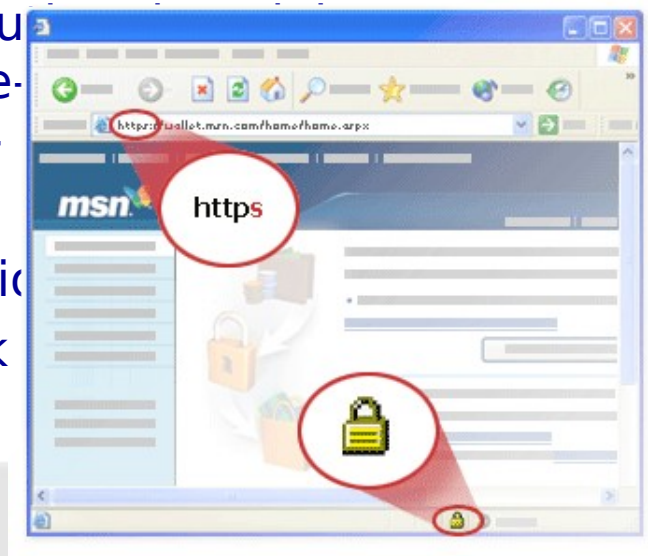
Credit for Phishing examples:
Washington Post, 2005

Phishing Safeguards

Simple Steps For Protecting Yourself

Just as they do in the physical world, scam artists will continue to develop new and more sin wa to trick you online. Here are five st that help protect from getting “hooked.”

1. Never respond to requests for personal information via e-mail or in a pop-up window. If in doubt, call the institu to be the sender of the e-
2. Visit Web sites by typing the URL into your address bar.
3. Check to make sure Web site uses encrypti
4. Routinely review your credit card and bank statements.
5. Report suspected abuses of your personal information to the proper authorities.



Avoiding Identity Theft – Other Safeguards

Reduce the risk of being a victim of identity theft by taking the following precautions:

- Buy a shredder
- Get your credit report
- Protect Your Social Security Number
- Make sure Your SSN isn't on your driver's license
- Keep your mother's maiden name between you and I

If you are victimized:

- Notify three big credit bureaus
- Close or suspend compromised accounts
- File police report
- Complain to FTC

Online Shopping

- The Internet is always open – seven days a week, 24 hours a day – and bargains ca numerous online
- Keep the following tips in mind to help ensu that your online shopping experience is a safe one
  - Shop with companies you know
  - Or do a background check if merchant is unfamiliar
    - Look for physical address
    - Call a company representative
    - Look for a third-party seal of approval such as Trust-e or
    - Check privacy and return policies
  - Keep your password(s) private
  - Submit credit card details and other personal information only over secure sites (https in address bar and padlock icon on bottom bar)
  - Pay by credit or charge card
  - Keep a record

Children on the Internet

- Unfortunately, sexual exploitation of children via the Internet does happen
- FBI created its *Innocent Images National Initiative* to stop online exploitation
  - 28 of 56 field offices have undercover operations
  - 200 FBI Agents work these cases
  - 10,000 cases since 1995 with nearly 3,000 convictions

Signs That Your Child May Be at Risk

FBI's *Parent's Guide to Internet Safety* says your child may be at risk on-line if you see the followir

- Your child spends large amounts of time on-l especially at night
- You find pornography on your child's comput
- Your child receives phone calls from men you don't know or is making calls to numbers you don't recognize
- Your child receives mail, gifts, or packages from someone you don't know
- Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room
- Your child becomes withdrawn from the family

Improving Your Child's Web Safety

Microsoft offers the following ideas of what to discuss with kids:

- Encourage your kids to share their Internet experience with you.
- Teach your kids to trust their instincts and tell you ab anything that makes them nervous.
- Choose login names that do not reveal personal information for chat rooms, instant messaging, and other on-line activities that require login names.
- Insist that your kids never give out your address, phone, or other personal information.
- Teach your kids that the difference between right and wrong is the same on the Internet as it is in real life.
- Show your kids how to respect others online.
- Insist that your kids respect the property of others online including copyrights.
- Tell your kids that they should never meet online friends in person.
- Teach your kids that not everything they read or see online is true.
- Control your children's online activity with advanced Internet software. Parental controls can help you filter out harmful content and monitor the sites your child visits.

Summary – Reviewing the Risk Model

- Risk is a function of assets, threats and vulnerabilities …

Risk = Asset * Threat * Vulnerability

PC: Efficiency
Data/files

Yourself: Privacy
Identity
Credit
Confidence

Family: Child
Safety

Viruses/Worms/Trojans SPAM
SpyWare
Phishing
Identity Theft
Shopping Scams
Online Predators

No Firewall
No Anti-virus
Unpatched SW
Unsafe Practice

As you have seen, nearly all safeguards available to us for reducing risk are those that reduce or eliminate a vulnerability, especially in the area of unsafe practices.

Summary – Recap of Safe Computing Practices

- Install anti-virus software and update the pattern files at least one a week.
- Install personal firewall software
- Check for security patches and updates to Windows operating system and program
- Install a spyware elimination tool
- Use a pop-up blocking utility if you wish
- Be suspicious of e-mail attachments
- Don’t trust displayed file names – can verify via Properties
- Set browser security setting to High
- Know what you are downloading from the Internet
- Encourage children to practice safe computing

Resources

Additional information about safe computing is available at the following resources, which were used in this presentation:

- Federal Trade Commission advice at http://www.ftc.gov/bcp/menu-internet.htm
- DFAS Safe Computing Zone on DFAS ePortal (IT Community) at https://eportal.dfas.mil/content/Technology%20Services/Infrastructure/safecomputing/index.htm
- Microsoft Security Home Page at http://www.microsoft.com/security/default.mspx
- DoD Enterprise-licensed antivirus and firewall software available for home use (free to DoD civilians and active military) at http://www.cert.mil/
- *Zone Alarm* (free version) personal firewall is available at: http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp?lid=zadb_zadown
- *Spybot Search and Destroy* spyware filter is available at: http://www.safer-networking.org/en/download/index.html
- Spamwasher SPAM filter ($30) is available from http://www.panicware.com/product_spamwasher.html
- *McAfee Internet Security Suite* comprehensive package can be purchased for $50 at http://www.networkassociates.com/us/buy/
- *Norton Internet Security* comprehensive package can be purchased for $70 at http://www.symantec.com/purchase/
- FBI Innocent Images Website at http://www.fbi.gov/hq/cid/cac/innocent.htm
- FBI Parent's Guide to Internet Safety at http://www.fbi.gov/publications/pguide/pguide.htm

Stay Safe and Be Happy!

DFAS

Your Financial Partner @ Work